

Serial No.: 09/650,177

Docket No.: F-190

REMARKS

Page 1 of the specification has been amended to make a specific reference to refer to the prior applications from which priority is claimed (as indicated on the PTO/SB/05 form filed on August 29, 2000).

As a preliminary matter, Applicants noted that the PTO-1449 form submitted with an Information Disclosure Statement filed on August 29, 2000 was not initialed and returned by the Examiner. Applicants respectfully request the references cited in this IDS be considered and the PTO-1449 form be initialed and returned with the next communication.

Claims 35 and 36 are pending in this application. Claims 35 and 36 were rejected under 35 U.S.C. §103(a) as being unpatentable over Fisher (U.S. Patent No. 5,005,200) in view of Payne et al. (U.S. Patent No. 5,715,314). Reconsideration is respectfully requested.

The present invention is directed to a secure user certification system for electronic commerce that provides an accounting system for services provided. In electronic commerce, various parties conduct activities without face to face contact. As such, it is desirable for each party to any transaction to be able to determine and verify the authenticity of the other party to the transaction, as well as ensure sufficient security for any commerce conducted electronically. Such security services could include, for example, message integrity, message authentication, message confidentiality, and message non-repudiation. In an electronic commerce environment these security services are achieved by cryptographic techniques such as digital signature, hash codes, encryption algorithms, and the like. To effectively implement the above, a party to an electronic commerce transaction requires access to a secure cryptographic device capable of securely implementing these cryptographic techniques. According to the present invention, a certificate meter provides certificate management services including use of cryptographically secured certificates. Payment for the processing and issuing, by the certificate authority, of

Serial No.: 09/650,177

Docket No.: P-190

the electronic certificates, also referred to as electronic postmarks, can be made using funds stored in the meter. Thus, the present invention provides a party to an electronic commerce transaction access to a secure cryptographic device, i.e., a certificate meter, associated with a certificate authority, while providing the certificate authority with a convenient payment system to allow the certificate authority to get paid for processing and issuing of the electronic certificates (postmarks).

In view of the above, claim 35 is directed to a method for "obtaining a cryptographic certificate" that comprises the steps of "providing a register having funds stored therein; determining if sufficient funds are present in the register for obtaining the certificate; sending a certificate request to a certificate authority; receiving the cryptographic certificate from the certificate authority; and deducting funds from the register for obtaining the requested certificate."

Fisher is directed to a public key cryptographic system with enhanced digital signature certification that authenticates the identity of the public key holder. Specifically, in Fisher, a trusted authority creates a digital message which contains the claimant's public key and the name of the claimant and a representative of the authority signs the digital message with the authority's own digital signature. This digital message, often referred to as a certificate, is sent along with the use of the claimant's own digital signature. Any recipient of the claimant's message can trust the signature, provided that the recipient recognizes the authority's public key. (Col. 3, lines 53-64). The system of Fisher provides the ability to specify a variety of attributes associated with the certification, such as specifying the authority or constraints which are conferred on the certifee by the certifier. (Col. 4, lines 56-62).

Thus, while Fisher discloses the use of certificates for providing security functions, as noted by the Office Action, there is no disclosure, teaching or suggestion in Fisher of providing payment to the certificate authority for processing and issuing the certificate.

To overcome the above deficiency, the Office Action relies on the reference to Payne et al. Payne et al. is directed to network-based sales system that includes at

Serial No.: 09/650,177

Docket No.: F-190

least one buyer computer for operation by a user desiring to buy a product, at least one merchant computer, and at least one payment computer. The computers are interconnected by a computer network. A purchase transaction begins when a user at buyer computer 12 requests advertisements (step 24) and buyer computer 12 accordingly sends an advertising document URL (universal resource locator) to merchant computer 14 (step 26). The merchant computer fetches an advertising document from the advertising document database (step 28) and sends it to the buyer computer (step 30). The user browses through the advertising document and eventually requests a product (step 32). This results in the buyer computer sending payment URL A to the payment computer (step 34).

The payment computer sends a payment confirmation document to the buyer computer, the payment confirmation document including an "open" link and a "continue" link (step 44). The confirmation document asks the user to click on a "continue" button if the user already has an account with the payment computer, or to click on an "open" button if the user does not already have an account and wishes to open one. If the user clicks on the "open" button (step 46), the buyer computer sends payment URL C to the payment computer (step 48), payment URL C being similar to payment URL A but also indicating that the user does not yet have an account. The payment computer creates a new account document (step 50) and sends it to the buyer computer (step 52). If the user clicks on the "continue" button (step 60), the buyer computer sends payment URL B to the payment computer (step 62), payment URL B being similar to payment URL A but also indicating that the user already has an account. The payment computer then instructs the buyer computer to provide the account name and password (steps 64 and 66), and the buyer computer prompts the user for this information by creating an account name prompt (example shown in FIG. 8) and a similar password prompt. The user enters the information (step 68) and the buyer computer sends the account name and password to the payment computer (step 70). The payment computer checks the settlement database to determine whether the user has unexpired access to the domain identifier contained in the payment URL (step 82). If so, the payment computer sends to the buyer computer a document providing an option either to repurchase or

Serial No.: 09/650,177

Docket No.: F-190

to use the previously purchased access (step 84). The user can respond to the recent purchase query document by choosing to access the previously purchased document (step 85) or to go ahead and buy the currently selected product (step 86). If the user chooses to buy the currently selected product, the payment computer calculates an actual payment amount that may differ from the payment amount contained in the payment URL (step 87). For example, the purchase of a product in a certain domain may entitle the user to access other products in the domain for free or for a reduced price for a given period of time. The payment computer then verifies whether the user account has sufficient funds or credit (step 76). If not, the payment computer sends a document to the buyer computer indicating that the user account has insufficient funds (step 78). (Col. 5, line 16 to Col. 7, line 20).

Thus, if Payne et al. teaches anything at all, it is merely a conventional network base sales system that utilizes a credit card account to pay for purchases made on-line. Note Fig. 7 of Payne et al. that illustrates a screen snapshot of a new account document that the payment computer sends to the buyer computer. The buyer must complete this document to make a purchase utilizing the system of Payne et al. As illustrated, the user must input a credit card number and expiration date, and also indicate if they are the owner of the credit card. The user must also provide an account name and password that will be linked to the credit card account. (See Col. 6, lines 15-42). If the user already has an account, the user must provide the account name and password which were previously associated with the buyer's credit card when the account was opened.

The Office Action states that it would have been obvious to combine Fisher and Payne et al. to arrive at the present invention, since by having an independent payment computer (e.g. a bank) verify a user's ability to pay prior to completing a transaction a merchant, such as a certificate authority, can guarantee compensation for service rendered. The present invention, however, is not directed to having an independent payment computer verify a user's ability to pay. As noted above, the present invention is directed to a certificate meter that can issue cryptographic certificates and provide payment for issuing the certificate. This is accomplished by

Serial No.: 09/650,177

Docket No.: P-190

providing a register having funds stored therein from which payment will be made upon receipt of the certificate. Even if Fisher and Payne et al. were combined, the combination still would not disclose, teach or suggest "providing a register having funds stored therein; determining if sufficient funds are present in the register for obtaining the certificate" and "deducting funds from the register for obtaining the requested certificate" as is recited in claim 35. As noted above, the only type of account disclosed in Payne et al. is a conventional credit card account. This is not the same as providing a register having funds stored therein. The combination of Fisher and Payne et al. would merely lead to a conventional credit card transaction. This is not the same as the present invention.

The fact that the present invention was made by the Applicants does not make the present invention obvious; that suggestion or teaching must come from the prior art. See C.R. Bard, Inc. v. M3 Systems, Inc., 157 F.3d 1340, 1352 (Fed. Cir. 1998). See, e.g., Uniroyal, Inc. v. Rudkin-Willey Corp., 837 F.2d 1044, 1051-1052 (Fed. Cir. 1988) (it is impermissible to reconstruct the claimed invention from selected pieces of prior art absent some suggestion, teaching, or motivation in the prior art to do so). "Determination of obviousness can not be based on the hindsight combination of components selectively culled from the prior art to fit the parameters of the patented invention. There must be a teaching or suggestion within the prior art, or within the general knowledge of a person of ordinary skill in the field of the invention, to look to particular sources of information, to select particular elements, and to combine them in a way they were combined by the inventor." ATD Corp. v. Lydall, Inc., 159 F.3d 534, 545 (Fed. Cir. 1998) (emphasis added). No such suggestion or motivation has been provided by the Office Action to arrive at the present invention from these references.

Without using the present claims as a road map, it would not have been obvious to make the multiple, selective modifications needed to arrive at the claimed invention from these references. The rejection uses impermissible hindsight to reconstruct the present invention from these references. See Ex parte Clapp, 227

serial No.: 09/650,177

Docket No.: P-190

U.S.P.Q. 972,973 (Bd. App. 1985) (requiring "convincing line of reasoning" to support and obviousness determination).

For at least the above reasons, Applicants respectfully submit that claim 35 is allowable over the prior art of record.

Claim 36, dependent upon claim 35, is allowable along with claim 35 and on its own merits.

In view of the foregoing remarks, it is respectfully submitted that the claim of this case is in a condition for allowance and favorable action thereon is requested.

Respectfully submitted,



Brian A. Lemm
Reg. No. 43,748
Attorney for Applicants
Telephone (203) 924-3836

PITNEY BOWES INC.
Intellectual Property and
Technology Law Department
35 Waterview Drive
P.O. Box 3000
Shelton, CT 06484-8000

Serial No.: 09/650,177

Docket No.: F-190

MARKED VERSION TO SHOW CHANGES**In The Specification:**

Page 1, before "Field of the Invention", add the following paragraph:

— This application is a divisional application of Serial No. 09/133,706, filed Aug. 13, 1998, now U.S. Patent No. 6,134,328, which is a continuation application of Serial No. 08/518,404, filed Aug. 21, 1995, now U.S. Patent No. 5,796,841.—